DUMPSBOSS.

Network Defense Essentials (NDE) Exam

ECCouncil 112-51

Version Demo

Total Demo Questions: 9

Total Premium Questions: 94

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Network Security Fundamentals	13
Topic 2, Identification, Authentication, and Authorization	11
Topic 3, Network Security Controls - Administrative Controls	5
Topic 4, Network Security Controls - Physical Controls	6
Topic 5, Network Security Controls - Technical Controls	12
Topic 6, Network Security Protocols	8
Topic 7, Network Security Devices	11
Topic 8, Wireless Network Security	6
Topic 9, Network Security Policies	5
Topic 10, Data Security	17
Total	94

QUESTION NO: 1

A network defender reviews web-server logs and finds hundreds of requests from one source IP address for URLs such as `/admin`, `/backup`, `/old`, and `/test`. Most requests return HTTP 404 responses, and there is no evidence that the attacker successfully authenticated.

Which stage of a cyberattack is most clearly indicated by this activity?

A. Reconnaissance

B. Unauthorized access

C. Denial-of-service

D. Data exfiltration

ANSWER: A

Explanation:

Reconnaissance is correct because the repeated requests for common administrative, backup, and test paths indicate an attempt to discover exposed resources and identify potential entry points. The attacker is gathering information about the web server before attempting to exploit a discovered weakness or use valid credentials.

Unauthorized access would require evidence that the attacker obtained access to a protected resource or account. A denial-of-service attack would focus on exhausting availability through high-volume or malformed traffic, rather than enumerating likely application paths. Data exfiltration involves transferring information out of the organization, which is not shown by the failed requests.

QUESTION NO: 2

A company maintains daily backups of a critical database. During a recovery test, administrators discover that the most recent backup file is corrupted and cannot be restored. Management requires a backup strategy that provides an additional independent copy so that a failure affecting the primary backup repository does not prevent recovery.

Which of the following backup principles should the company implement?

A. Increase the frequency of backups in the same repository

B. Implement the 3-2-1 backup rule

C. Use RAID instead of maintaining backups

D. Keep only one backup copy at an offsite location

ANSWER: B

Explanation:

The **3-2-1 backup rule** is correct because it recommends maintaining at least three copies of data, stored on two different types of media, with one copy kept offsite. This approach reduces the risk that corruption, hardware failure, ransomware, or a site-specific incident will affect every available copy.

Simply increasing the frequency of backups may create more recovery points but does not ensure independence from the failed repository. RAID improves availability of storage hardware but is not a substitute for backups because replicated corruption or deletion can affect all disks. Retaining only one offsite copy still leaves the organization without multiple independent recovery options.

QUESTION NO: 3

During an investigation of suspected data theft, a security analyst copies relevant firewall logs and a disk image from an employee workstation. The organization expects the evidence may be used in disciplinary proceedings. The analyst records the date and time, calculates a hash value for each collected file, documents every person who receives the evidence, and stores the originals in a locked evidence cabinet.

Which of the following practices is demonstrated by the analyst in the above scenario?

A. Chain of custody

B. Log retention

C. Incident reporting

D. Data masking

ANSWER: A

Explanation:

Chain of custody is correct because the analyst documents the collection, handling, transfer, and storage of the evidence. Recording who possessed the evidence and when establishes accountability, while hashing helps demonstrate that the collected files have not been altered. Secure storage protects the originals from unauthorized access or modification.

A forensic image is a copy of data, but it does not by itself document subsequent handling. Log retention preserves records, and incident reporting communicates findings, but neither provides the documented evidence-handling history required in this scenario.

QUESTION NO: 4

A company places finance workstations and guest wireless devices on separate VLANs. Users in the guest VLAN must access the Internet but must not communicate with finance systems, even when they are connected to the same physical switch infrastructure.

Which of the following controls best enforces this requirement?

A. Configure an ACL on the inter-VLAN routing device

B. Configure a trunk port between the VLANs

C. Enable port security on all guest access ports

D. Assign the same IP subnet to both VLANs

ANSWER: A

Explanation:

An **access control list (ACL) on the inter-VLAN routing device** is correct because separate VLANs create distinct Layer 2 broadcast domains, but traffic can still pass between them if a router or Layer 3 switch is configured to route between the VLANs. An ACL can explicitly deny guest-VLAN traffic to the finance subnet while allowing the traffic required for Internet access.

Creating the VLANs alone does not guarantee that inter-VLAN communication is blocked once routing is enabled. A trunk port carries traffic for multiple VLANs between network devices and does not implement the required access restriction. Port security controls which devices may connect to a switch port, but it does not provide subnet-to-subnet traffic filtering.

QUESTION NO: 5

Which of the following techniques protects sensitive data by obscuring specific areas with random

characters or codes?

A. Data retention

B. Data resilience

C. Data backup

D. Data masking

ANSWER: D

Explanation:

Data masking is correct because it protects sensitive information by replacing, hiding, or altering selected data elements so that the original values are not exposed to unauthorized users. For example, a payment-card number can be displayed as a partially concealed value, or a real name, account identifier, or health record field can be substituted with realistic but non-sensitive characters or values. This allows organizations to use data in contexts such as software development, testing, analytics, demonstrations, and customer-support workflows without unnecessarily revealing the underlying confidential information. Masking may be static, where a protected copy is created for nonproduction use, or dynamic, where the displayed value is masked according to the viewer's authorization while the original remains protected in the source system. Effective masking techniques preserve an appropriate format and usability while reducing the likelihood that sensitive data can be read or misused. The National Institute of Standards and Technology describes data masking as a privacy-enhancing technique that obscures sensitive data while supporting authorized business use. Additional implementation guidance is available from the NIST Guide for De-Identifying Government Datasets and the OWASP Data Masking resource.

QUESTION NO: 6

A network administrator deploys a firewall at the Internet perimeter. The firewall permits outbound web traffic only after it verifies that the traffic belongs to an established connection initiated from the internal network. Unsolicited inbound packets that do not match an existing connection are dropped.

Identify the type of firewall employed in the above scenario.

A. Packet-filtering firewall

B. Stateful inspection firewall

C. Proxy firewall

D. Next-generation firewall

ANSWER: B

Explanation:

A **stateful inspection firewall** is correct because it maintains a state table containing details of active connections, such as source and destination addresses, ports, and TCP session state. It can therefore determine whether an inbound packet is a valid response to an internal connection or an unsolicited attempt to begin a new connection.

A packet-filtering firewall can make decisions using individual packet header fields, but it does not inherently track the state of a connection. A proxy firewall intermediates application communications, while a next-generation firewall adds capabilities such as application awareness and deep inspection. The decisive feature in this scenario is validation against an established connection state.

QUESTION NO: 7

An organization hosts its public website on a server with a private IP address in an internal network. External users must reach the website through a public IP address, but the organization does not want to assign public addresses directly to internal servers.

Which of the following network address translation techniques should be configured?

A. Dynamic NAT

B. Port forwarding

C. Port address translation (PAT)

D. Split tunneling

ANSWER: B

Explanation:

Port forwarding is correct because it maps traffic received on a specific public IP address and port, such as TCP port 443, to the private address and service port of an internal server. This allows Internet users to reach the public website while the server retains its private internal address.

Dynamic NAT creates temporary address mappings from an address pool, and PAT commonly allows many internal clients to share one public address for outbound connections. Static NAT provides a fixed one-to-one address mapping, but the scenario specifically requires publishing a particular web service through a public address and port. Port forwarding is the appropriate technique for that requirement.

QUESTION NO: 8

Bob has secretly installed smart CCTV devices (IoT devices) outside his home and wants to access the recorded data from a remote location. These smart CCTV devices send sensed data to an intermediate device that carries out pre-processing of data online before transmitting it to the cloud for storage and analysis. The analyzed data is then sent to Bob for initiating actions.

Identify the component of IoT architecture that collects data from IoT devices and performs data pre-processing.

A. Streaming data processor

B. Gateway

C. Data lakes

D. Machine learning

ANSWER: B

Explanation:

Gateway is correct because an IoT gateway serves as the intermediate layer between endpoint devices, such as smart CCTV cameras, and cloud-based services. It receives or aggregates telemetry, video metadata, and other sensed data from local IoT devices, often translating between device protocols and IP-based cloud communications. Crucially, gateways can perform edge processing before data leaves the local environment. This preprocessing may include filtering irrelevant events, validating or normalizing data, compressing data, buffering it during connectivity interruptions, and applying basic rules or analytics. Processing data nearer to the cameras reduces bandwidth consumption and latency, while allowing the cloud platform to focus on durable storage, larger-scale analytics, and centralized management. In the scenario, the device that receives sensed CCTV data, preprocesses it online, and then transmits it to cloud storage and analysis is therefore an IoT gateway. NIST describes edge computing as processing performed near the data source, a role commonly implemented by gateways in IoT deployments. AWS similarly identifies IoT gateways as components that connect devices and can process data locally before forwarding it to cloud services. See NIST Edge Computing Concepts, Approaches, and Applications and AWS Overview of Internet of Things.

QUESTION NO: 9

Which of the following tools is designed to identify and prevent malicious Trojans or malware from infecting computer systems or electronic devices?

A. HOIC

B. HitmanPro

C. Hulk

D. Hashcat

ANSWER: B

Explanation:

HitmanPro is correct because it is an antimalware tool designed to identify malicious software on endpoints, including Trojans, viruses, spyware, ransomware, rootkits, and other potentially unwanted or malicious programs. It uses behavior-based detection and cloud-assisted scanning to evaluate suspicious files, enabling it to detect threats that may evade a system's primary security product. This makes it useful as a second-opinion scanner when an organization or user suspects an existing antivirus solution may have missed an infection.

In addition to detecting malicious artifacts, HitmanPro supports remediation by identifying and removing detected malware, helping return an infected computer to a safer operating state. Its purpose aligns directly with endpoint malware defense: preventing malicious code from remaining active and reducing the likelihood that malware can compromise data, credentials, system integrity, or network resources. Sophos, the vendor associated with HitmanPro, describes the product as a malware removal tool and documents its scanning and cleanup role. For product details, see Sophos HitmanPro. For broader guidance on protecting systems from malware through preventive controls and detection, see CISA's malware guidance.